MARKED UP COPY OF AMENDMENT PURSUANT TO 37 CFR § 1.121 (b)(1)(iii)

Page 1, line 4 to page 1, line 8.

BACKGROUND [OF THE INVENTION]

[Field of the Invention]

This [invention] disclosure relates to controlling the access of computer information accessible by a computer system.

[Description of the Related Art]

Page 1, line 21 to page 2, line 19.

Both individuals and organizations utilize computer systems to provide access to computer information. The computer information accessible by a computer system may be stored in the computer system such as in a hard disk drive or accessible by the computer system via a computer network or a peripheral device. Consequently, it is desirable to restrict access to that information. Past techniques of controlling access include utilizing passwords for logging on to a computer system or network. Another technique for determining authorized access includes utilizing smart card readers (e.g., magnetic or optical) to read smart cards or other physical objects that include encoded identification information. An example of such a system can be found in Bilich et al., U.S. Pat. No. 5,877,483, entitled “Method and Apparatus for Automatically Implementing Computer Power On and Logon Functions Using Encoded ID Card,” having a common Assignee, which is hereby incorporated by reference in its entirety. Another example can be found in Bouthillier et al., U.S. Pat. 5,894,552, which is hereby incorporated by reference in its entirety. Other examples techniques for controlling access are found in a patent application entitled "Portable Computer System With Hierarchical and Token-Based Security Policies, serial number 09/237,016, and having a common Assignee, which is hereby incorporated by reference in its entirety.

Other techniques for determining whether a user has authorized access include the utilization of biometric identification such as by the analysis of fingerprints, eye, or voice patterns. An example of such a system can be found in [the patent application] U.S. Patent 5,838,306, entitled "Mouse With Security Feature," having [a filing] an issue date of [August 20, 1997] November 17, 1998, [a serial number of 08/914,948,] listed inventors Clint O'Conner and Erica Scholder, and a common Assignee, all of which is hereby incorporated by reference in it's entirety.

Page 3 line 3 to page 5 line 13

SUMMARY [OF THE INVENTION]

It has been discovered that a wireless identification signal sent by an identification object can be utilized in controlling access to computer information accessible by a computer system. One advantage of such a system is that it can be configured to place the computer system in a higher power state from a lower power state without requiring the performance of a conscious access action of a user, thereby reducing the amount of time required for logging onto the system. Another advantage is that the system can be configured to deny access to computer information accessible by the computer system when the identification signal has not been received for a predetermined period of time.

In one aspect, the [invention] disclosure includes a computer system having at least one processor and an identification signal detection circuit for receiving a wireless identification signal from an identification object. The wireless identification signal contains identification information regarding the assigned processor of the identification object. The computer system also includes a memory having means for determining whether the assigned possessor of the identification object as indicated by the wireless identification signal has authorized access to computer information accessible by the computer system. The computer system further includes a memory having means for determining that the identification signal detection circuit has not received for a predetermined period of time, a wireless identification signal containing identification information from an assigned possessor having authorized access.

In another aspect, the [invention] disclosure includes a method for controlling access to computer information. The method includes sending a wireless identification signal by an identification object. The wireless identification signal includes identification information regarding an assigned possessor of the object. The method includes receiving, independent of a conscious access action by a user, the wireless identification signal by a detection circuit. The method further includes determining whether the assigned possessor as indicated by the wireless identification signal has authorized access to computer information accessible by a computer system. The method still further includes granting access to computer information accessible by the computer system if determined that the assigned possessor as indicated by the wireless identification signal is authorized access.

In another aspect [of the invention], an identification object for an assigned possessor includes a circuit having a controller, an antennae, and a memory operably coupled to the connector. The memory has means for generating an information signal periodically broadcast via the antennae. The information signal contains identification information regarding the assigned possessor.

BRIEF DESCRIPTION OF THE DRAWINGS

The present [invention] disclosure may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

Figure 1 is a perspective view of one example of a computer system and an identification object [according to the present invention].

Figure 2 is a perspective view of one example of an identification object that includes a block diagram of a transmitting circuit [according to the present invention].

Figure 3 is a block diagram of one example of a detection circuit [according to the present invention].

Figure 4 is a block diagram of one example of a computer system [according to the present invention].

Figure 5 is one example of a state diagram utilized in controlling access to computer information [according to the present invention].

Figure 6 is one example of a state diagram utilized in controlling access to computer information [according to the present invention].

The use of the same reference symbols in different drawings indicates identical items.

DETAILED DESCRIPTION

The following sets forth a detailed description of a mode for carrying out the [invention] embodiments. The description is intended to be illustrative of the [invention] disclosure and should not be taken to be limiting.

Figure 1 is a perspective view of an example of a computer system and an identification object [according to the present invention]. Computer system 101 is a personal computer that includes a stand alone chassis 113, a monitor 109, and a keyboard 111. Computer system 101 can provide a user access to computer information such as, e.g., computer information stored in a hard disk drive (481 in Figure 4) installed in chassis 113, or stored in other computer systems accessible by computer system 101 over a network (not shown) such as a local area network or a wide area network.

Page 6, line 16 to page 7, line 9.

In some embodiments, computer system 101 utilizes the power management strategy of computer system 101 in controlling access to computer information. Power management strategies were developed by the computer industry to reduce the amount of power consumed by computer systems. Typically, power management strategies are utilized to shut down or turn off various devices and features of the computer system via hardware of software mechanisms when the computer system is not in use. An example of one power management strategy is the ADVANCED POWER MANAGEMENT (APM) Interface Specification, developed by INTEL™, and MICROSOFT™. Another is the ADVANCED CONFIGURATION AND POWER INTERFACE (ACPI) specification by INTEL™, MICROSOFT™, and TOSHIBA™. These specifications define power states at which the computer system may reside. The power states of a power management strategy typically range from the highest state, where the computer system is operating normally in an on power state such as where the computer system can process data, to the lowest state where the computer system is completely turned off. Various devices of the computer system are shut down and the system processor may not perform computations at lower intermediate power states. Such intermediate power states include the Standby, Suspend, and Hibernation power states for the APM specification and the Sleeping and Soft-off power states for ACPI specification. A further explanation of such power management strategies is found in U.S. Patent Application entitled "Prevention of Power State Change in Response to Chassis Intrusion," having a serial number of 09/322,296, listed inventors Terry L. Matula and John R. Stuewe, a filing date of May 28, 1999, and a common assignee, which is hereby incorporated by reference in its entirety.

Page 7, line 28 to page 8, line 10.

Access to the computer information in a locked state may be restricted by utilizing any of a number of conventional access restriction techniques. For example, some computer systems have the capability to restrict access to computer information located on a non volatile storage device of a computer system. An example of such a system is found in the patent application entitled "Portable Computer Systems With Hierarchical and Token-Based Security Policies," having a serial number 09/237,016. For such systems, receipt of a wireless identification containing identification information of an authorized user may be required for access to the restricted information. Also, a wireless identification signal may contain other information needed for enabling access to restricted data. For example, the identification signal may contain decoding information for unscrambling data stored in a computer system that implements data encryption to restrict access.

Page 8, line 27 to page 9, line 9.

Figure 2 shows one example of an identification object that includes a transmitting circuit [according to the present invention]. Transmitting circuit 121 is embedded in badge 110 with the outer dimensions of badge 110 shown in phantom on Figure 2. Transmitting circuit 121 includes an integrated circuit chip 202 having a controller 205 and a memory circuit 213 for storing code that controller 205 executes for performing its operation. Transmitting circuit 121 also includes an embedded antennae 211 for broadcasting a wireless identification signal and an embedded battery 210 for power. Because battery 210 is embedded in Figure 2, badge 110 is thrown away when battery 210 is fully discharged. However with other badges, the battery may be replaceable or rechargeable. Additionally, the transmitting circuit may be powered by other techniques such as with a solar cell. Other transmitting circuits may include other circuitry or may have other forms or configurations.

Page 9, line 21 to page 10, line 12.

The Bluetooth Specification is set forth as one example of a wireless protocol that may be utilized for transmitting an identification signal by transmitting circuit 121. Those of skill in the art will recognized that, based upon the teachings herein, a transmitting circuit [according to the present invention] may utilize other wireless protocols for transmitting the identification information and other information.

Figure 3 sets forth an example of a detection circuit [according to the present invention]. Detection circuit 114 is mounted on add-in card 115 that is inserted into a computer bus connector (see Figure 4) to operably couple detection circuit 114 to system processor (402 in Figure 4). Detection circuit 114 includes a controller 305, a receiver circuit 307, a memory circuit 309, and an antennae 319 for receiving an identification signal. Controller 305, receiver circuit 307, and memory circuit 309 are operably coupled together via bus 315. Detection circuit 114 also includes a bus interface circuit 311 which enables detection circuit 114 to be operably coupled to a computer bus. In Figure 3, bus interface circuit 311 conforms to the PCI Local Bus Specification. Detection circuit 114 also includes I/O pins for providing an #PME signal and receiving a +3.3 Vaux signal which will be discussed later. Detection circuit 114 is powered by an auxiliary power supply (not shown) that provides power even when computer system 101 is in a soft off power state. Other detection circuits [according to the present invention] may have other forms or configurations. For example, some or all of the circuits of detection circuit 114 shown in Figure 3 may be integrated on a single chip.

Page 10, line 25 to page 11, line 4.

Figure 4 is a block diagram of computer system 101 [according to the present invention]. Computer system 101 includes a system processor 402 such as, e.g., the PENTIUM III processor sold by INTEL™. RAM 409 is operably coupled to system processor 402 via a memory hub controller (MCH) 405, which in one embodiment is implemented with the 440BX chipset sold by INTEL™. A video controller 410 conforming to the Advanced Graphics Port Specification (AGP video controller) is mounted on a computer card (not shown) that is inserted into an AGP card slot connector 411 which is operably coupled to memory control hub 405 via AGP bus 412.

Page 18, line 4 to page 18, line 5.

Other computer systems according to the present [invention] disclosure may implement state diagrams having other configurations.

Page 19, line 20 to page 19, line 25.

While particular embodiments of the present [invention] disclosure have been shown and described, it will be recognized to those skilled in the art that, based upon the teachings herein, further changes and modifications may be made without departing from this [invention] disclosure and its broader aspects, and thus, the appended claims are to encompass within their scope all such changes and modifications [as are within the true spirit and scope of this invention].

MARKED UP COPY OF AMENDED CLAIMS 4-7, 16, 19, 21, 28 AND 35 PURSUANT TO 37 CFR § 1.121 (c)(1)(ii)

4. (Amended) The computer system of claim 3 [further comprising:] wherein placing the computer system in a condition to deny further includes placing the computer system in a lower power state in response to the identification signal detection circuit not having received for a predetermined period of time, a wireless identification signal containing identification information from an assigned possessor having authorized access.

5. (Amended) The computer system of claim 3 [further comprising:] wherein placing the computer system in a condition to deny further includes logging a user off of the computer system in response to the identification signal detection circuit not having received for a predetermined period of time, a wireless identification signal containing identification information from an assigned possessor having authorized access.

6. (Amended) The computer system of claim 3 [further comprising:] wherein placing the computer system in a condition to deny further includes placing the computer system in a locked state in response to the identification signal detection circuit not having received for a predetermined period of time, a wireless identification signal containing identification information from an assigned possessor having authorized access.

7. (Amended) The computer system of claim 3 [further comprising:] a memory circuit storing operating system code whose execution by the at least one processor implements an operating system for controlling the operation of the computer system; and

wherein the operating system code includes code whose execution places the computer system in a condition to deny access to computer information accessible by the computer system in response to the identification signal detection circuit not having received for a predetermined period of time, a wireless identification signal containing identification information from an assigned possessor having authorized access.

16. (Amended) The computer system of claim 1 wherein:

the identification signal detection circuit has an output to provide an indication signal indicating that the identification signal detection circuit has received a wireless identification signal containing identification information of an assigned possessor of a security object determined to have authorized access; and

wherein the identification signal is provided in response to receiving a wireless identification signal containing identification information of an assigned possessor of a security object determined to have authorized access after a predetermined period of time of not receiving an identification signal containing identification information of an assigned possessor of a security object determined to have authorized access.

19. (Amended) The computer system of claim 1 further comprising:

a memory having means for implementing a state machine including at least one state of a first state type and at least one state of a second state type;

wherein in a state of the first state type, the identification signal detection circuit is receiving identification signal containing identification information of an assigned possessor having authorized access within a predetermined period of time from a previously received identification signal containing identification information of the assigned possessor having authorized access; and

wherein in state of the second state type, the identification signal detection circuit is not receiving an identification signal containing identification information of an assigned possessor having authorized access within a predetermined period of time from a previously received identification signal containing identification information of the assigned possessor having authorized access.

21. (Amended) A method for controlling access to computer information comprising:

sending a wireless identification signal by an identification object, the wireless identification signal including identification information regarding an assigned possessor of the object;

receiving, independent of a conscious access action by a user, the wireless identification signal by a detection circuit;

determining whether the assigned possessor as indicated by the wireless identification signal has authorized access to computer information accessible by a computer system; and

granting access to computer information accessible by the computer system if determined that the assigned possessor as indicated by the wireless identification signal is authorized access.

28. (Amended) The method of claim 21 wherein the granting access further includes:

displaying on a user interface a message requesting a user to provide a password;

determining whether the password provided by the user is assigned to the assigned possessor determined to have authorized access; and

granting access to computer information assessable by the computer system if determined that the password is assigned to the assigned possessor.

35. (Amended) An identification object for an assigned possessor comprising:

a circuit including:

a controller;

an [antennae] antenna; and

a memory operably coupled to the connector, the memory having means for generating an information signal periodically broadcast via the [antennae] antenna, the information signal containing identification information regarding the assigned possessor.

REMARKS

Minor changes have been made to the specification. Claims 4-7, 16, 19, 21, 28 and 35 are amended and Claims 1-37 remain in the application.

Entry of this amendment to the specification and claims prior to Examination is courteously solicited.

No new matter is added by the amendments herein.

Respectfully submitted,

James R. Bell
Registration No. 26,528

Dated: 8-16-02
HAYNES AND BOONE, L.L.P.
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 512/867-8407
Facsimile: 512/867-8470

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Non-Fee Amendment, Commissioner For Patents, Washington, D.C. 20231

on 8/16/02
Date

Signature

Nisih PASANYA
Typed or Printed name of person signing Certificate

A-136031.1